(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
21 December 2006 (21.12.2006)

(10) International Publication Number
WO 2006/134226 A1

(51) International Patent Classification:
H04L 12/58 (2006.01)

(21) International Application Number:
PCT/FI2006/050251

(22) International Filing Date: 12 June 2006 (12.06.2006)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20055306 13 June 2005 (13.06.2005) FI

(71) Applicant *(for all designated States except US)*: DELTAGON GROUP OY [FI/FI]; Lauttasaarentie 48 B, FI-00200 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: KOISTINEN, Pasi [FI/FI]; Kivenlahdenkatu 3 H 91, FI-02320 Espoo (FI).

(74) Agent: PATENT AGENCY COMPATENT LTD.; Hitsaajankatu 6, FI-00810 Helsinki (FI).

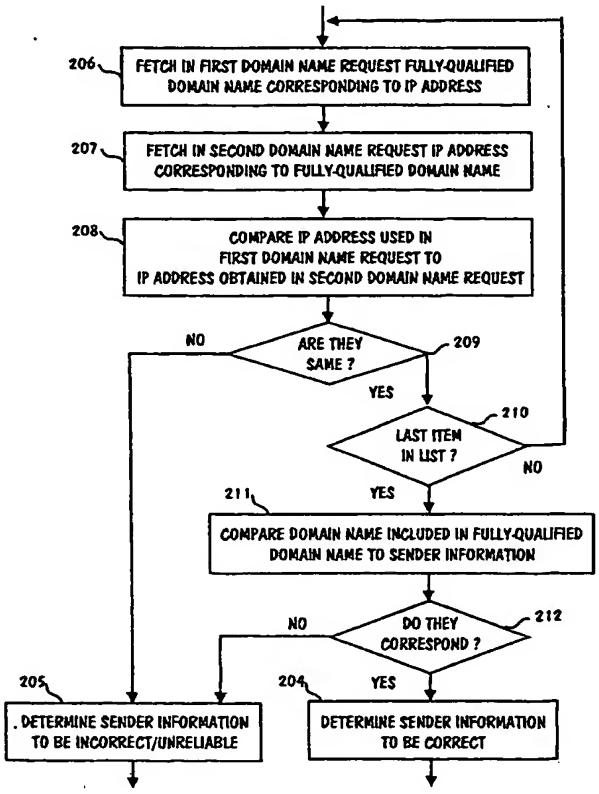
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SERVER FOR AUTHENTICATING SENDER OF EMAIL AND NOTIFYING EXCHANGE INFORMATION OF EMAIL



(57) Abstract: The invention includes a method for authenticating a sender of an email. The method examines items of the transmission information of the email, i.e. the items located in 'Received' fields are examined starting from an item of transmission information that is entered in the email by a server preceding the server that received the email. The transmission information ('Received' fields) is examined until either an unreliable item of the transmission information is found or the all items of the transmission information are handled by a so-called "Reverse IP verification" method. When the all items of the transmission information are handled, the item of the transmission information that is at first entered in the email is examined in a check. In this check a domain name obtained in 'Reverse IP verification' method is compared to a domain name included in the sender information of the email. If the domain names correspond to each other, the sender of the email has been successfully authenticated. In addition, the invention includes an email server utilizing the method.

WO 2006/134226 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and server for authenticating sender of email and notifying exchange information of email

Field of the invention

The invention relates generally to the security of electronic mail (email) and especially to the possibilities by which the recipient of an email can ensure that the sender information entered in the email is reliable.

Background of the invention

The Internet comprises a number of servers, routers, and other so-called nodes and communication links connecting the nodes. Typically, emails pass through multiple Internet nodes from a sender to a recipient. When sending an email the sender doesn't usually know through which nodes the email will pass. Each node through which the email passes may take a copy for itself or the node may forward the message or the copy of it to another node. For this reason, unencrypted email is considered to be a comparatively insecure communication method.

A recipient of a conventional email cannot surely know whether the sender entered in an email is really sent the email or is the sender someone else.

Email is usually transmitted through the Internet by using a protocol termed SMTP (Simple Mail Transfer Protocol) that is specified in the IETF (Internet Engineering Task Force) specification: RFC822. In addition, the SMTP protocol has been developed with an extension (RFC3207) concerning so-called SSMTP (Secure SMTP) by means of which a sending server and a receiving server can communicate each other in a secured way.

In the following it is described a traditional way according to the, SMTP protocol for handling an email when the email is sent from server *A* to server *B*:

(A=sending server, B=receiving server)

1) B> 220 ESMTP ready
2) A> helo smtp.domain.tld
3) B> 220 Hello.
4) A> MAIL From:<sender@domain.tld>
5) B> 220 sender ok

6) A> RCPT TO:<recipient@domain.tld>
7) B> 220 recipient ok
8) A> DATA
9) B> 220 Enter data followed by <CR><LF>.<CR><LF>
10) A> From: sender@domain.tld
11) A> To: recipient@domain.tld
12) A> Subject: Message Subject
13) A>
14) A> The actual message
15) A>.
16) B> 250 Ok
17) A> QUIT
18) B> 220 Bye.

Before, in Phases 1-3, servers *A* and *B* perform a handshaking.

In Phases 4-7, the routing information of the email is transmitted. The routing information determines a recipient of the email. So-called return address is determined in the routing information for a situation in which the email cannot be delivered.

In Phases 8-16 the email is transmitted from one server to another. Phases 8 and 9 prepare the transmission.

In Phases 10-12 the header information which is separated from the actual message with a blanc line (Phase 13) is transmitted.

In Phase 14 the actual message, i.e. the text and possible attachment files, are transmitted. The server *A* sends a line including a dot (.) and a line feed (Phase 15). After Phase 15 the receiving server *B* usually stores the message in its disk.

In Phase 16 server *B* sends an acknowledgement that the message has been received. Servers *A* and *B* terminate the connection (Phases 17 and 18). Hereafter the sending server *A* usually removes the email from its disk.

Thus, the previous example describes the operation of two servers (*A* and *B*). The servers transmitting the email may be parts of a long chain. Therefore the transmission of the email through this chain comprises a number of times Phases 1-18. In the following a server can be also be termed "a router".

"Chaining" of the routers/servers that transmit email causes a transmission delay, because a following router in the chain cannot transmit an email until when the previous router has transmitted the email as a whole. In addition, the email is frequently stored in each router on the disk of the router, which increases the transmission delay.

It is possible to transmit the email so that a server belonging to the chain contacts a following server of the chain immediately when it has adequate items of information for the email transmission.

In the above example server *B* has the adequate information after Phase 8 in order that it can contact the following server (server *C*). Then the message transmission through the chain of routers (*A*, *B*, *C*) will be accelerated, because the following router (router *C*) is able to transmit the message simultaneously when the previous router (server *B*) is still receiving the end part of the message from the first router of the chain (server *A*). This type of transmission for email is termed a "transparent message transmission". The transparent message transmission includes a benefit that the first router (server *A*) obtains an item of information from the last router (server *C*) immediately when the message is transmitted to its recipient. In addition, the transparent message transmission reduces the risk of losing a message when a server which is located in the middle of the chain (server *B*) is broken during the message transmission.

Generally speaking, the routers may be physical routers or virtual routers. A number of virtual routers can be placed inside one physical router.

FIG. 1 shows a server that includes virtual routers. A server 101 receives a message 102 in accordance with a protocol (SMTP) and transmits the message 102 forward. The server 101 includes four routers which are termed: an email firewall 103, a security proxy 104, a content filter 105, and an SMTP back-end 106. Arrows drawn between the routers 103-106 describe how the message 102 moves inside the server 101 from a router to another. If the traditional transmission method is used, each router 103-106 stores the message 102 on a disk of the server 101. If the transparent message transmission is used instead of the traditional transmission method the message 102 is not stored on the disk, but the router 103-105 immediately forwards the message 102 and don't send an acknowledgement of the message reception before the following router 104-106 sends the acknowledgement of the message reception.

An open-source software Amavisd which is downloadable in the Internet implements the transparent routing inside a server.

The transparent routing between servers is related to challenges, because an SMTP email (message) may have a number of recipients and the email addressed to them maybe routed via different servers. Then a router obeying the transparent message transmission needs to divide the transmission of the email to number of servers, which complicates the management of the transmission. Thus, the transparent message transmission operates best in the reception of the email, i.e. in the last server of "the chain" or in the virtual servers placed inside a server.

The following authentication problem is related to the prior art: everyone can send with whatever sender address email via the Internet. In addition, complicated transmission chains make more difficult to find out the real origin of the email, because each physical server, and many times also virtual servers included in servers, make their own notations to headers of the emails. An unreliable server may make additional notations to the header and this way try to conceal the real origin of the email.

One solution to the authentication problem is to use digital signing in emails. However, only few senders and recipients of emails use it. Digital signing requires software installations at the terminals of the senders and the recipients. A sender signs his/hers message by means of the software and the recipient checks whether the signature attached to the message is unique or not.

Another solution which is more developed than the previous one is to use a specific server for creating digital signatures and for checking them. Then the origin of emails can be checked, for example, at the organization level.

Certain methods have been developed to authenticate a server transmitting an email.

'Reverse IP verification' is a known method for authenticating the server which has sent/transmitted the email. In the following the function of the 'Reverse IP verification' method is described.

Let us assume that the name of a receiving server is 'domain-b' and the IP address of a sending server is 123.45.67.89. Then the receiving server 'Domain-b' makes the following notation to the transmission information:

Received: from smtp.domain.tld (smtp.domain.tld [123.45.67.89])
by smtp.domain-b.tld with ESMTP

In the first phase of the 'Reverse IP verification' method the receiving server performs a DNS query in which the server, i.e. 'Domain-b', requests from the domain name server (DNS) the domain name corresponding to the above-mentioned IP address:

dig @dns-server1 PTR 89.67.45.123.in-addr.arpa

As response to the DNS query the DSN (dns-server1) returns, for example, the following reply:

89.67.45.123.in-addr.arpa PTR smtp.domain.tld

The reply of the DNS discloses that the IP address 123.45.67.89 corresponds to a fully-qualified domain name 'Domain'.

In the second phase of the 'Reverse IP verification' method it is find out the fully-qualified domain name that corresponds to the IP address 123.45.67.89. Then 'Domain-b' server uses another DNS server (dns-server2) as shown in the following DNS query:

dig @dns-server2 A smtp.domain.tld.

As response to the DNS query the DNS (dns-server2) returns, for example, the following reply:

smtp.domain.tld. A 123.45.67.89

Finally, 'Domain-b' server compares the IP address 123.45.67.89 entered in the Received field to the IP address 123.45.67.89 obtained in the second phase of the 'Reverse IP verification' method. In this example the IP addresses are the same, i.e. the message is sent from the server whose domain name is 'Domain' and whose IP address is 123.45.67.89.

'Reverse IP verification' method is generally known in many router applications, for example, 'Postfix' (www.postfix.org) uses it.

Let us assume as in the above example that the domain name 'Domain' and the IP address 123.45.67.89 correspond to each other. Then 'Domain-b' server enters to the message header the domain name 'Domain' in parentheses and the IP address 123.45.67.89 in brackets.

Let us assume that 'Domain-b' server forwards the received message, for example, to 'Domain-c' server.

In addition, let us assume that the fully-qualified domain name of 'Domain-b' server is 'smtp.domain-b.tld' and the IP address of 'Domain-b' server is 234.56.78.90. Then 'Domain-c' server enters in the message header the following item of information:

Received: from smtp.domain-b.tld (smtp.domain-b.tld [234.56.78.90])
by smtp.domain-c.tld with ESMTP

wherein ESMTP is an acronym from the words "Enhanced Simple Mail Transport Protocol".

After this the message includes the following transmission information:

Received: from smtp.domain-b.tld (smtp.domain-b.tld [234.56.78.90])
by smtp.domain-c.tld with ESMTP
Received: from smtp.domain.tld (smtp.domain.tld [123.45.67.89])
by smtp.domain-b.tld with ESMTP

For example, 'Postfix' router application enters in the transmission information as described above.

In addition to the 'Reverse IP verification' method there are other known methods by which it is find out the trustworthiness of the servers participating in sending or transmitting of a message. One of these messages uses a list that includes the IP addresses of trusted servers. If the IP address of a transmitting server is found in the list, the transmitting server is

considered to be reliable (enough). If the transmitting server is not found in the list of trusted servers, the server is considered to be unreliable.

The other known methods for authenticating a transmitting server are SPF (Sender Policy Framework) and Microsoft Sender ID. In these methods any organization sending email publishes in a domain name service an item of information that discloses from which email server the emails related to the domain name are sent. By means of the SPF or 'Microsoft Sender ID' method, for example, the following targets can be defined as certified email servers: a) a single IP address, b) all IP addresses that are related to a domain name, and/or c) so-called "MX servers" related to the domain name. So-called 'Best guess' method is an extension to the SPF method. In 'Best guess' method it possible to assume that the all IP addresses and/or the all MX servers of the domain name are reliable, although the organization sending the email is not published any DNS information according to the method.

It is also known that the server can enter an identifier in the header of an email so that the sender of the email can be identified by means of the identifier.

It is also known that the correctness of the sender information of the email is ensured by sending a so-called check message to the sender of the email. This type of methods based on use of a check message are described, for example, in the US patents 6,393,465 and 6,868,498. A weakness of these methods is an additional diligence which they cause to a sender, because the sender needs to handle the check message/messages related to his/hers email.

Another problem related to the prior art is how to express the transmission method of email.

One way to express the transmission method of email is used in UNIX mail servers. In this mode of expression the sender information of a message is changed when the message arrives from the Internet to an organization so that the recipient (an end user) of the message is able to separate the messages coming inside the organization from the messages coming from the Internet. The sender information is changed so that in the start of it is placed, for example, a notation 'EXT'. Then the sender information of the message looks like this, for example:

EXT Matti Virtanen matti.virtanen@konsemi.tld

A corresponding notation can also be entered in the subject field of the message.

A third problem related to the prior art technique is that the technique requires additional actions for a sending organization. If the sending organization doesn't have any authentication method in use, the sending server cannot be authenticated, except when using 'Best guess' method within the SPF method. However, 'Best guess' method is a quite unreliable way to authenticate a sender of an email, because the email may be received though a very complicated transmission chain.

A third problem related to the prior art concerns the above-mentioned SPF method. The problem appears in a situation in which a message is sent outside of an organization and a server used by the organization is defined to transmit the message to a recipient located outside of the organization. If the recipient uses the SPF method, the SPF method results in that the origin entered in the message is wrong, because on the basis of its 'envelope from' address the message should come from another server than the server outside of the organization to which the message was transmitted to the recipient.

Summary of the invention

The main objective of the invention is to solve the above-mentioned problems related to the prior art.

An email transmitted though the Internet may pass via a number of servers/routers to a recipient, whereat the email typically includes the transmission information entered by each server participated in the transmission of the email.

The invention comprises a method for authenticating a sender of an email, the email including transmission information written by at least one server (router). The method in accordance with the invention utilizes the above-described 'Reverse IP verification' method. In more detail, the transmission information is examined by means of 'Reverse IP verification' method, i.e. the information of 'Received' field is examined starting from the transmission information which a server preceding the server that received the email has entered in the email. The transmission information ('Received' fields) is passed through until an unreliable item of the transmission information is found or the all items of the transmission information are

handled by the 'Reverse IP verification' method. In the last case it is performed a check addressed to an item of the transmission information which is first entered in the email. In this check the fully-qualified domain name obtained by 'Reverse IP verification' method is compared to the domain name included in the sender information of the email. If the domain names correspond to each other the sender of the email is authenticated. If needed, the examination performed by the method can be accomplished with 1-4 additional checks.

In addition to the method, the invention comprises a server which is equipped with the checking means and sends and/or transmits emails.

Brief description of the drawings

The invention is described more closely with reference to the accompanying drawings, in which

Figure 1 shows a server that includes virtual routers,
Figure 2A shows an operation principle of the method,
Figure 2B shows the examination steps performed in the method,
Figure 3 shows editing a list to be used in the examination,
Figure 4A shows an additional examination step in which the start of a domain name is evaluated by a heuristic method,
Figure 4B shows another additional examination step in which the domain name is searched in the list of captured servers,
Figure 4C shows another additional examination step in which MX information is utilized,
Figure 4D shows another additional examination step in which a RIPE database is utilized,
Figure 5 shows a server in accordance with the invention.

Detailed description of the invention

The method is thus related to authenticating a sender of an email. The authentication of a sender means generally that the sender entered in the email is the actual sender of the email. In other words, the sender of the email can sufficiently enough to trust that the email is from the sender entered in the 'From' field.

The authentication of the server also includes checking the correctness of the transmission information. These items of the transmission information disclose the servers through which the email has passed from the original sender to the recipient.

Method is also related to how the transmission manner of the email can be disclosed in the header of the email in a better way than nowadays. The method replaces the items included in the header of the email with checked items of the information on the basis of which it is possible to estimate the trustworthiness of the origin of the email. In more detail, the email application or another application makes a notation in the address field of the original sender on the basis of which the end user knows that the origin of the email has not been successfully verified. The notation made in the address field may include, for example, three questions marks [???] placed in the brackets.

In addition, the possible encryption can be disclosed to the end user with a certain notation placed in the address field of the sender. For example, the notation indicating the use of encryption may be '.S'.

In order to save time of end users, the application operating according to the method can be implemented so that the application classifies the received emails to two different folders on the basis of the trustworthiness of the origin of the emails.

It is known in the prior art that an email server writes the text "unknown" in the header of an email and it writes the IP address of the email in brackets, if the 'Reverse IP verification' method discloses that the fully-qualified domain name and the IP address of the email don't correspond to each other.

It is essential from the point of view of the invention which checks are performed for an email and when the email is determined to be correct.

Let us assume that the transmission information included in the email is the following:

Received: from smtp.domain-b.tld (smtp.domain-b.tld [234.56.78.90])
by smtp.domain-c.tld with ESMTP
Received: from smtp.domain.tld (smtp.domain.tld [123.45.67.89])
by smtp.domain-b.tld with ESMTP

Let us also assume that the sender information of the email is:

From: matti.meikalainen@domain.com

Lets us describe the operation of the method by means of the following example. The transmission information and the sender information shown above are examined as follows.

1) The last item of the transmission information is read, i.e. a notation of 'Received' field is read by a server preceding the server which received the email and made the notation.

2) Extracting the IP address from the item of the transmission information, for example, the IP address 34.56.78.90.

3) Checking whether the IP address obtained in Step 2 is found on the list of reliable servers.

4) If it is not found, the IP address is written in the list.

5) If it is found, Steps 2-4 are performed for the next item of the transmission information. If the read item of the transmission information is the first item written in the email, the next step is Step 6.

6) Reading the IP address from the list.

7) Finding out the fully-qualified domain name by means of a DNS search ('smtp.domain.tld', in this example).

8) Finding out the IP address corresponding to the fully-qualified domain name by means of a DNS search (34.56.78.90, in this example).

9) If the IP address read from the list and the IP address returned by the DNS search are the same, Steps 6-8 are performed for the next item entered in the list. If the read IP address is the last one in the list, the next step is Step 10.

10) Separating from the fully-qualified domain name corresponding to the IP address the end part of the domain name ('domain.tld', in this example).

11) Examining whether the end part of the fully-qualified domain name corresponds to the sender information of the email, i.e. the end part of the fully-qualified domain name included in 'From' field.

12) If they correspond to each other, the sender is authenticated.

The following remark is related to Step 4: the IP address included in the item of the transmission information which is first entered in the email is always written in the list.

The method discloses from which organization the email is coming from. The method operates even if there is in the middle a server in public use, for example, a server of an Internet operator, providing that this "middle server" writes its own 'Received' line in the email.

FIG. 2A shows an operation principle of the method. The method is intended for authenticating the sender of an email at the server which received the email. It is formed 201 in the server a list of those items of transmission information which at least one server participating in the transmission of the email has entered in the email. Then the list is examined 202 starting from an item of the transmission information entered in the email by a server preceding the server which received the email. The examination includes at least the steps shown in FIG. 2B. The examination indicates whether 203 the examined items of the information are reliable. If they are, the sender information entered in the email is determined 204 to be correct at the server received the email.

FIG. 2B shows the examination steps of the method which are performed in the all embodiments of the method. This examination to be performed by a server which received the email is based on a list composed of items of transmission information of the email ('Received' field) and the sender information of the email ('From' field). The examination is started from the item of the transmission information entered in the email by a server preceding the server received the email. The examination comprises the following steps. In the first domain name request 206 it is fetched the fully-qualified domain name corresponding to the IP address entered in the item of the transmission information. In the second domain name request 207 it is fetched the IP address corresponding to the fetched fully-qualified domain

name. Then the IP address used in the first domain name request is compared 208 to the IP address obtained in the second domain name request. If the compared IP addresses are the same and the item of the transmission information is the last one in the list 210, the domain name fetched in the first domain name request is compared 211 to the sender information of the email. The email includes the domain name related to the sender of the email. If the domain names correspond to 212 each other, the sender information of the email is determined 204 to be correct. Thus, the sender information is determined to be correct when the list composed of the items of the transmission information is passed through and in the comparison 209 those items are verified be reliable, and in the comparison 212 the sender information is verified be reliable/correct. If the list still includes items not examined 210, the following item is read from the list and at least the steps 206-208 are performed. If the comparison 209 discloses that the IP addresses are not the same, the sender information is determined 205 to be incorrect.

FIG. 3 shows editing the list to be used in the examination. The editing of the list means that the following step is performed between the steps 201 and 202 shown in FIG. 2A. Each such item of the transmission information, which a server to be found in the list of reliable IP addresses has entered in the email, is removed from the list by the server received the email. A notation made by a reliable server is trusted in such extent that the notation, i.e. the item of the transmission information is not examined. When the list including the items of the transmission information becomes shorter, also the execution time required by the method becomes shorter. For example, the list of reliable IP addresses can be composed of a company's or a community's own servers. Then all other servers are interpreted to be 'unreliable', i.e. the items of the transmission information entered by them remain in the list and those items are examined according to FIG. 2A.

If needed, the accuracy of the examination can be enhanced by the additional steps shown in FIGs 4A - 4D. The additional steps are targeted to the above-mentioned list that includes the items of the transmission information ('Received' fields).

FIG. 4A shows the additional examination step in which the start of a domain name is examined by a heuristic method. In more detail, at the server which received the email a part of the fully-qualified domain name is

examined 401 by means of the specified heuristic method. This part remains when two character strings separated by a dot are removed from the end of the domain name which was fetched in the first domain name request 206. The heuristic method indicates whether the part discloses a dynamic network address or non-dynamic network address. Let us assume that according to the examination 401 the part, which remains when two character strings separated by a dot are removed from the end of the domain name, discloses a non-dynamic network address. If the item is the last one in the list 210 and the domain names compared in step 212 correspond to each other, the sender information ('From' field) is determined to be correct. Forgery or capture of a non-dynamic network addresses is much more difficult than the forgery or capture of a dynamic network addresses. Alternatively, if the part discloses on the basis of the examination 401 a dynamic network address, the item of the transmission information is determined to be incorrect/unreliable and therefore the sender information ('From' field) is determined to be incorrect/ unreliable 205.

In addition or alternatively, the examination shown in FIG. 2B can be improved with the following additional step.

FIG. 4B shows the additional examination step in which the domain name is searched in the list of captured servers. This step is preferably performed when the 'Reverse IP verification' is finished (FIG. 2, step 209). Some Internet servers transmitting emails are captured by unwanted parties, such as hackers. The captured servers, or in more detail, their domain names are entered in the lists which are generally available. Those lists can be considered to form one logical list. In FIG. 4B, at server which received the email, the domain name is searched 403 in the (logical) list of captured servers. After this, the sender information is determined 404 to be correct, if the searched domain name is missing from the list of captured servers and if the domain name is the last item of the transmission information (in the list including 'Received' fields) 210 and the compared domain names correspond to each other 212.

In addition or alternatively, the examination shown in FIG. 2B can be improved with the following additional step.

FIG. 4C shows the additional examination step in which MX (Mail eXchange) information is utilized. The MX information is stored in a domain name server (DNS). An item of the MX information discloses to which server

the emails addressed to certain domain name are to be delivered. In step 405 the following sub-steps are performed: 1) using the fully-qualified domain name obtained in the first domain name request as a search key, the search resulting in MX (Mail eXchange) information, 2) using at least one fully-qualified domain name included in the MX information in a domain name request, and some of the fully-qualified domain names included in the MX information resulting in the domain name request an IP address which corresponds to the IP address entered in the item of the transmission information 406, 3) determining the item of the transmission information to be correct. If the item of the transmission information determined to be correct is the last one in the list 210 and the on the basis of the comparison 211 the domain names correspond to each other 212, the sender information ('From' field) is determined to be correct.

Alternatively, even after the step 204 an additional check utilizing MX information can be targeted to the sender information.

In this additional check the following sub-steps are performed: 1) using a domain name related to the sender as a search key in a search, the search resulting in the MX information, 2) comparing the fully-qualified domain name which corresponds to the IP address entered in the item of the transmission information to at least one fully-qualified domain name included in the MX information, and if the compared fully-qualified domain name corresponds to some fully-qualified domain name included in the MX information, 3) determining the sender information to be correct.

In addition or alternatively, the examination shown in FIG. 2B can be improved with the following additional step.

FIG. 4C shows the additional examination step in which MX (Mail eXchange) information is utilized. The MX information is stored in a domain name server (DNS). An item of the MX information discloses to which server the emails addressed to certain domain name are to be delivered. In step 405 the domain name fetched in step 206 is compared to the MX information obtainable through the domain name service of the Internet. If the domain name corresponds 406 to some item of the MX information, the item of the transmission information is determined to be correct. If the item of the transmission information is the last one in the list 210 and the domain names correspond to each other 212, the sender information ('From' field) is determined to be correct.

In addition or alternatively, the examination shown in FIG. 2B can be improved with the following additional step.

FIG. 4D shows the additional examination step in which RIPE (Réseaux IP Européens) database is utilized. As described above, the IP address corresponding to the fetched domain name is fetched in the second domain name request 207. In the additional step 407 this IP address is used as a search key when searching in the RIPE (WHOIS) database the owner organization related to the IP address. In the additional step 408 the information disclosing the owner organization is compared to the domain name obtained in the first domain name request 206. If the owner organization information corresponds 409 to the domain name, the item of the transmission information is reliable. Otherwise, the item of the transmission information is unreliable and the sender information is determined to be incorrect/unreliable.

The method in accordance with the invention is related to a number of embodiments. In one embodiment the sender information of the email is determined to be correct only when the additional steps 401, 403, 405, 407, and 408 shown in FIGs. 4A – 4D indicate that the all items of the transmission information are correct and in step 212 the domain names correspond to each other. In all other cases the sender information of the email is considered to be incorrect.

In the other embodiments of the method the determination of the correctness of the email is performed in another way. First, the number of the additional steps to be performed may vary, for example, only the additional step 401 shown in FIG. 4A is performed. Secondly, the sender information can be determined to be correct, even if some additional step indicates that an item of the transmission information is incorrect.

It is possible to attach a degree of safety to the sender information. The degree of safety is, for example, an integer number between 0-100 so that 0 means the sender information to be definitely incorrect and 100 means the sender information to be definitely correct. The degree of the security can be implemented, for example, by giving points so that each of the additional steps 401, 403, and 405 results in 0-20 points, the additional steps 407 and 408 result in together 0-20, and the step 212 results in 0-20 points. Then the degree of safety is the sum of the points, i.e. an integer number between 0-

100. It is possible to define a threshold value, for example, 80 which must be received in order that the sender information is determined to be correct.

In a certain embodiment of the invention the degree of safety related to the sender information of an email is stored through the domain name server of the Internet in a database of the degree of safety. The degree of safety is stored with the domain name and the IP address of the sender to the database of the degree of safety. Then it is possible to perform a search in the database when new emails are received from the IP address of the sender. If the degree of safety fetched from the database with the domain name and IP address is low, it is reasonable to take a suspicious attitude to the received emails.

It is also possible to attach the degree of safety to a server which transmitted the email. Then the degree of safety describes the trustworthiness of the server instead of the trustworthiness of the sender (the IP address of the sender). Then the degree of safety is increased when an email which is determined to be correct according to the method of the invention is received via the server. Correspondingly, the degree of the safety is degreased if the sender information of the email is determined to be incorrect.

A certain embodiment of the method includes a step of adding a server to the list of reliable IP addresses when, on the basis of the degree of safety, the server transmits with high probability emails having correct sender information. In more detail, the IP address of the server is added to the list of reliable IP addresses, which has been discussed in FIG. 3. Then also such situation is controlled in which an email is received from outside of an organization, but a server locating inside the organization is adapted to forward the received email to a recipient locating outside of the organization.

As a summary, the following aspects are mentioned. If needed, the method can be used without the additional checks shown in FIGs 4A – 4D. However, if at least one of the four additional checks is used, the sender of an email is determined to be correct, when the following three conditions are true: an item of the transmission information is the last one in the list 210, the domain name obtained in the first domain name request includes a domain name related to the sender of the email 212, and at least one additional check indicates that the item of the transmission information is correct. As described above, at the server which received the email, it is

possible to attach to the sender information the degree of security that defines the probability of the correctness of the sender information. The probability is higher the greater the number of performed additional check has indicated an item/items of the transmission information to be correct. In addition, it is possible to store a degree of safety with the sender information in a database or a memory for utilizing the degree of safety later on. At the server which received the email the degree of safety is preferably entered in the header of the email. Then the recipient of the email can himself/herself determine whether the sender information is correct or not.

A degree of safety is preferably entered in 'From' field. A degree of safety can also be entered in 'Reply To' field of the email.

In addition, it is possible to enter in 'From' and/or 'Reply To' a degree of strength of encryption. The degree of strength of encryption is another subject matter that a notation indicating use of encryption (for example, '.S'). The degree of strength of encryption discloses how strong/reliable encryption technique (or techniques) is used in the transmission of an email.

In order to define a degree of strength of encryption the method comprises the following steps in which 'sender information' related to the received email (the 'sender information' is not meant the sender information of a reply email), Usually, each server participated in the transmission of the email which uses regular post server software (e.g. Postfix) enters in the transmission information a notation about the use of the transmission information and the degree of strength of encryption. This item of information is normally not visible for the recipient of an email and neither does it disclose the real security level of the channel used for the email transmission. Conversely, if the items of transmission information which are determined to be reliable according to the method of the invention, it is possible to check whether the all reliable items of the transmission include information about encryption. It is possible to find out on the basis the notations about the degree of strength of encryption the strength of the incoming encryption for example, by selecting from the items of the transmission information the notation corresponding to the weakest degree of encryption). In the next step, the domain name included in the sender information is used in an MX query to be performed through the domain name service. This MX query results in a set of MX servers. Next, it is established to an MX server

(included in the set) an SMTP (Simple Mail Transfer Protocol) test connection that discloses whether the MX server supports the email encryption and which is the degree of strength of encryption. The degree of the outcoming encryption can be defined by choosing the weakest degree of the degrees of strength of encryption defined through the test connections to the MX servers related to the domain name. The degree of the incoming traffic encryption and the degree of the outcoming traffic encryption are separately entered in the header of email or, if needed, they can be combined to one degree of strength describing the overall level of encryption.

As a summary, the following aspects are mentioned. The method may enter in the header of an email (in 'From' field and/or in 'Reply To' field) at least one of the following notations: a) a notation of forgery disclosing that the sender information is determined to be incorrect, b) a notation of encryption disclosing that at least one encryption technique is used in the email transmission. In addition or alternatively, at least one of the following notations can be entered in the header of the email: c) degree of safety disclosing on which probability the sender information is correct, d) degree of strength of encryption.

Possible dissymmetry characters related to the transmission channel can be disclosed by using 'From' field as well as 'Reply-To' field for notifying the above-mentioned items of information a), b), c) and/or d). For example, if an email has arrived in a secured transmission manner, but the reply email would depart in an unsecured transmission manner, a notation indicating encryption is entered in 'From' field and the notation indicating encryption is omitted from 'Reply To' field.

An email application operating in a regular way is needed to transmit the notations a), b), c) and/or d) to the recipient of an email. When the recipient of the email (not the reply email) receives the email, the email application shows in 'From' field the text that includes the notations a), b), c) and/or d). When the email is replied, i.e. the reply email is sent, the email application operating in the regular way extracts a character string from 'Reply To' field to be used as the reply address. When the end of this character string includes the notations a), b), c) and/or d), those notations are transmitted to a sender of the reply email. In more detail, the sender of the reply email sees the notations in 'To' field of the reply email. On the basis of the notations the sender of the email can ascertain the correctness of the

recipient address and the transmission manner of the email. For example, if the email has arrived in a secured manner, but the reply email is going to depart in an unsecured way, the sender of the reply email is informed about this before sending the reply email. Then he/she can take into account this subject matter when considering the content of the reply email. The pure encryption of an email does create security, but the security is closely related to the correctness of recipient addresses (for example, the security is not created, if a well encrypted email is sent to an entirely wrong organization).

In addition to the method, the invention comprises a server for authenticating the sender of an email and notifying the exchange information of the email. The server is adapted to perform the steps of the method described above.

FIG. 5 shows a server in accordance with the invention. The server 501 is intended for authenticating the sender of an email 502. The server 501 receiving the email 502 includes means 503 for forming a list of those items of the transmission information which at least one server participated in the transmission of the email has entered in the email. In addition, the server 501 includes at least means for examining 505 and means for IP comparison 506. The method handles the list 504 with the means for examining 505 by starting from an item of the transmission information entered in the email by a server preceding the server received the email. The means for IP comparison 506 are used in handling the list. These means are adapted: a) to receive from the means for examining 505 an item of the transmission information, b) to fetch in a first domain name request a fully-qualified domain name corresponding to an IP address entered in the item of the transmission information, c) to fetch in a second domain name request an IP address corresponding to the fully-qualified domain name, d) to compare the IP address used in the first domain name request to the IP address obtained in the second domain name request, and when the compared IP addresses are the same e) to return the domain name to the means for examining 505. The means for examining 505 are adapted: f) to read a domain name related to the sender of the email, g) to compare the read domain name to the domain name returned by the means for IP comparison, and h) to determine the sender information to be correct when the compared domain names correspond to each other.

Thus, the server in accordance with the invention includes at least the means 503, 505, and 506. In addition to these, the server 501 may include other means, and the means for examining 505 may be adapted to perform other actions than the above-mentioned actions f), g) and h).

In order to speed up the handling of the list 504 the means for examining 505 are preferably adapted to remove from the list each such item of the transmission information which a server to be found in a list of reliable IP addresses has entered in the email. Then the list become shorter and the means for IP comparison 506 needs to be used less than before.

The server 501 may further include means for heuristics 507. These means are adapted to consider by using a heuristic method such a part of the domain name which remains when the last two character strings separated by a dot are removed from the end of the fully-qualified domain name. The means for IP comparison 506 fetched this fully-qualified domain name in the second domain name request.

If the server 501 includes the means for heuristics 507, the means for examining 505 are adapted to determine the sender information of the email 502 to be correct when the means for heuristics indicate that it is a non-dynamic network address.

If needed, the examining means 505 are further adapted search the domain name returned by the means for IP comparison 506 in a list of captured servers. Usually, the sender information of an email is determined to be correct only when each searched domain name is missing from the list of captured servers.

The examining means 505 are further adapted to perform the following actions: 1) to use the fully-qualified domain name obtained in the first domain name request as a search key, the search resulting in MX information, 2) to use at least one fully-qualified domain name included in the MX information in a domain name request, and 3) to determine the item of the transmission information to be correct, if some fully-qualified domain name included in the MX information results in the domain name request an IP address that corresponds to the IP address entered in the item of the transmission information.

If needed, relating to the additional check of the sender information, the examining means 505 are adapted to perform the following actions: 1) to use the domain name related to the sender information as a

search key in a search, the search resulting in MX information, 2) to compare the fully-qualified domain name which corresponds to the IP address entered in the item of the transmission information to at least one fully-qualified domain name included in the MX information, and 3) to determine the sender information to be correct, if the compared fully-qualified domain name corresponds to some domain name included in the MX information.

Relating to the additional check of the sender information the examining means 505 are further adapted to use in the IP address obtained in the second name server request as a search key when fetching information about an owner organization from the RIPE database and after that to compare the owner organization information obtained in the data base query to the domain name obtained in the first domain name request.

The server 501 preferably includes notation means 508 which are adapted to enter in the header information of the email at least one of the following notations: a) a notation of faulty indicating that the server has determined the sender information to be incorrect, b) a notation of encryption indicating that at least one encryption technique has been used when the email was transmitted through the Internet, c) a degree of safety disclosing in which probability the sender information is correct, or d) a degree of strength disclosing how strong encryption method is used in the transmission of the email. These notations are entered in the email which is transmitted by the server and which has the same content (the text and/or attachment files) as the email 502 received by the server.

In addition to the above-mentioned examples, there are other ways to implement the method and server in accordance with the invention. However, these ways are obvious for a person skilled in the art on the basis of his/her professional ability and the instructions obtainable from this patent application.

The invention is defined in the attached patent claims concerning the method and the server.

Claims

1. A Method for authenticating a sender of an email, the method being characterized in that at a server received the email

forming a list of items of transmission information which at least one server participating a transmission of the email has entered in the email,

examining the list starting from an item of the transmission information entered in the email by a server preceding the server received the email, the examination comprising the steps of

fetching in a first domain name request a fully-qualified domain name corresponding to an IP address entered in the item of the transmission information,

fetching in a second domain name request an IP address corresponding to the fully-qualified domain name,

comparing the IP address used in the first domain name request to the IP address obtained in the second domain name request, and when the compared IP addresses are the same

examining the next item of the transmission information,

when the item of the transmission information is the last item in the list,

comparing said fully-qualified domain name to a sender information of the email which includes a domain name related to a sender of the email, and

determining the sender information to be correct when the compared domain names correspond to each other.

2. The method as in claim 1 characterized in that before the examination

removing from the list each such item of the transmission information which a server to be found in a list of reliable IP addresses has entered in the email.

3. The method as in claim 1 characterized in that the method includes a first additional check in which

considering by means of a heuristic method such a part of the domain name fetched in the second domain name request which remains

when the last two character strings separated by a dot are removed from the end of the domain name, the heuristic method finding out whether said part discloses a dynamic network address or a non-dynamic network address, and when said address discloses the non-dynamic network address

determining the item of the transmission information to be correct.

4. The method as in claim 1 characterized in that the method includes a second additional check in which

searching a domain name in a list of captured servers and the domain name missing from the list of captured servers,

determining the item of the transmission information to be correct.

5. The method as in claim 1 characterized in that the method includes a third additional check in which

using the fully-qualified domain name obtained in the first domain name request as a search key, the search resulting in MX (Mail eXchange) information,

using at least one fully-qualified domain name included in the MX information in a domain name request,

and some of the fully-qualified domain names included in the MX information resulting in the domain name request an IP address which corresponds to the IP address entered in the item of the transmission information

determining the item of the transmission information to be correct.

6. The method as in claim 1 characterized in that the method includes an additional check targeted to the sender information in which

using a domain name related to the sender as a search key in a search, the search resulting in MX information,

comparing the fully-qualified domain name which corresponds to the IP address entered in the item of the transmission information to at least one fully-qualified domain name included in the MX information,

and if the compared fully-qualified domain name corresponds to some fully-qualified domain name included in the MX information,

determining the sender information to be correct.

7. The method as in claim 1 characterized in that the method includes a fourth additional check in which

using in the IP address obtained in the second name server request as a search key when fetching owner organization information from a RIPE database (RIPE WHOIS database),

comparing the owner organization information obtained in the database query to the domain name obtained in the first domain name request and when the domain names correspond to each other

determining the item of the transmission information to be correct.

8. The method as in claims 1-7 characterized in that determining in the method the item of the transmission information to be correct when the following conditions are true: a) the item of the transmission information is the last item of the transmission information, b) the domain name obtained in the first domain name request related to the item of the transmission information includes a domain name related to the sender of the email, and c) at least one performed additional check indicates that the item of the transmission information is correct.

9. The method as in claims 1-7 characterized in that a degree of safety describing a probability of correctness of the item of the transmission information is added at the server to the sender information, the probability being higher, the greater number of performed additional checks indicates the item/items of the transmission information to be correct.

10. The method as in claim 9 characterized in that at the server received the email

storing the degree of safety with the sender information in a memory.

11. The method as in claim 9 characterized in that at any server receiving the email

entering the degree of safety to the header information of the email

12. The method as in claim 1 characterized in that at any server receiving the email

entering to the header information of the email at least one of the following notations: a notation of faulty indicating that the sender information has been determined to be incorrect, a notation of encryption indicating that

at least one encryption technique has been used when the email was transmitted through the Internet.

13. The method as in claim 1 characterized in that the method includes following steps to be performed at any server receiving the email

using a domain name related to the sender information in an MX-query to be performed through the domain name service, the MX query resulting in a set of MX servers,

establishing an SMTP connection to each MX server included in the set, the SMTP connection disclosing whether the MX server supports encryption of email and when at least one MX server supports the encryption of email

entering in the header information of the email a degree of encryption indicating how strong encryption technique is usable for a reply message of the email.

14. A server for authenticating a sender of an email characterized in that a server includes

means for forming a list of those items of transmission information which at least one server participated in a transmission of the email has entered in the email received by the server,

means for examining the list by starting from an item of the transmission information entered in the email by a server preceding the server that received the email,

means for IP comparison which are adapted

to receive from said means for examining an item of the transmission information,

to fetch in a first domain name request a fully-qualified domain name corresponding to an IP address entered in the item of the transmission information,

to fetch in a second domain name request an IP address corresponding to the fully-qualified domain name,

to compare the IP address used in the first domain name request to the IP address obtained in the second domain name request, and when the compared IP addresses are the same,

to return the domain name to said means for examining,

said means for examining being adapted to

read a domain name related to the sender of the email,

examining the next item of the transmission information,

and in an association with the last item in the list composed of the items of the transmission information

to compare the read domain name to the domain name returned by the means for IP comparison and

to determine the sender information to be correct when the compared domain names corresponds to each other.

15. The server as in claim 14 characterized in that the means for examining are further adapted

to remove from the list each such item of the transmission information which a server to be found in a list of reliable IP addresses has entered in the email.

16. The server as in claim 14 characterized in that the server further includes means for heuristics which are adapted

to consider by means of a heuristic method such a part of domain name fetched in the second domain name request which remains when the last two character strings separated by a dot are removed from the end of the domain name, the heuristic method finding out whether said part discloses a dynamic network address or a non-dynamic network address.

17. The server as in claim 16 characterized in that the means for examining are further adapted

to determine the sender information to be correct when the examination performed by the means for heuristics indicates that said part discloses the non-dynamic network address.

18. The server as in claim 14 characterized in that the examining means are further adapted search the domain name in a list of captured servers.

19. The server as in claim 14 characterized in that the examining means are further adapted:

to use the fully-qualified domain name obtained in the first domain name request as a search key, the search resulting in MX information,

to use at least one fully-qualified domain name included in the MX information in a domain name request, and

to determine the item of the transmission information to be correct, if some fully-qualified domain name included in the MX information results in the domain name request an IP address that corresponds to the IP address entered in the item of the transmission information.

20. The server as in claim 14 characterized in that the examining means are further adapted:

to use the domain name related to the sender information as a search key in a search, the search resulting in MX information,

to compare the fully-qualified domain name which corresponds to the IP address entered in the item of the transmission information to at least one fully-qualified domain name included in the MX information, and

to determine the sender information to be correct, if the compared fully-qualified domain name corresponds to some domain name included in the MX information.

21. The server as in claim 14 characterized in that the examining means are further adapted

to use in the IP address obtained in the second name server request as a search key when fetching owner organization information from a RIPE database (RIPE WHOIS database) and

to compare the owner organization information obtained in the database query to the domain name obtained in the first domain name request.

22. The server as in claim 14 characterized in that the server further includes notation means which are adapted

to enter in header information of the email at least one of the following notations: a) a notation of faulty indicating that the server has determined the sender information to be incorrect, b) a notation of encryption indicating that at least one encryption technique has been used when the email was transmitted through the Internet, c) a degree of safety disclosing in which probability the sender information is correct, or d) a degree of strength disclosing how strong encryption method is used in the transmission of the email.

PRIOR ART

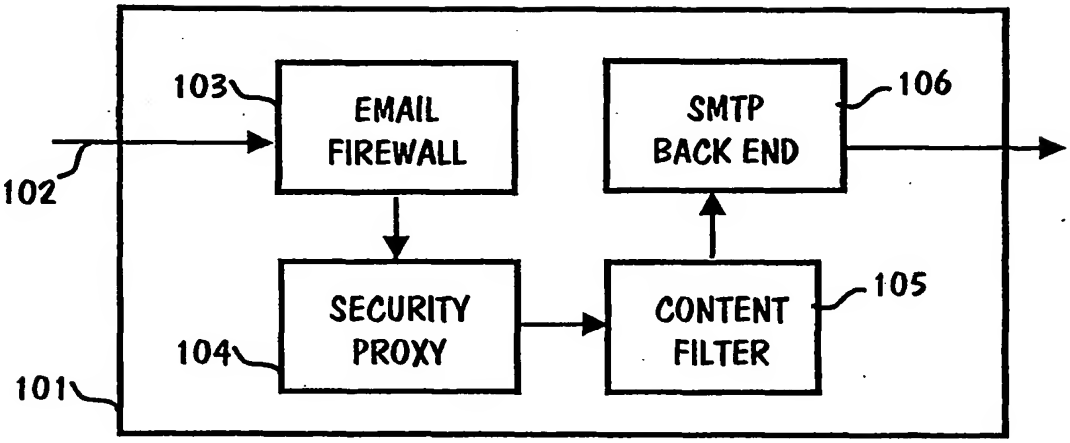


FIG. 1

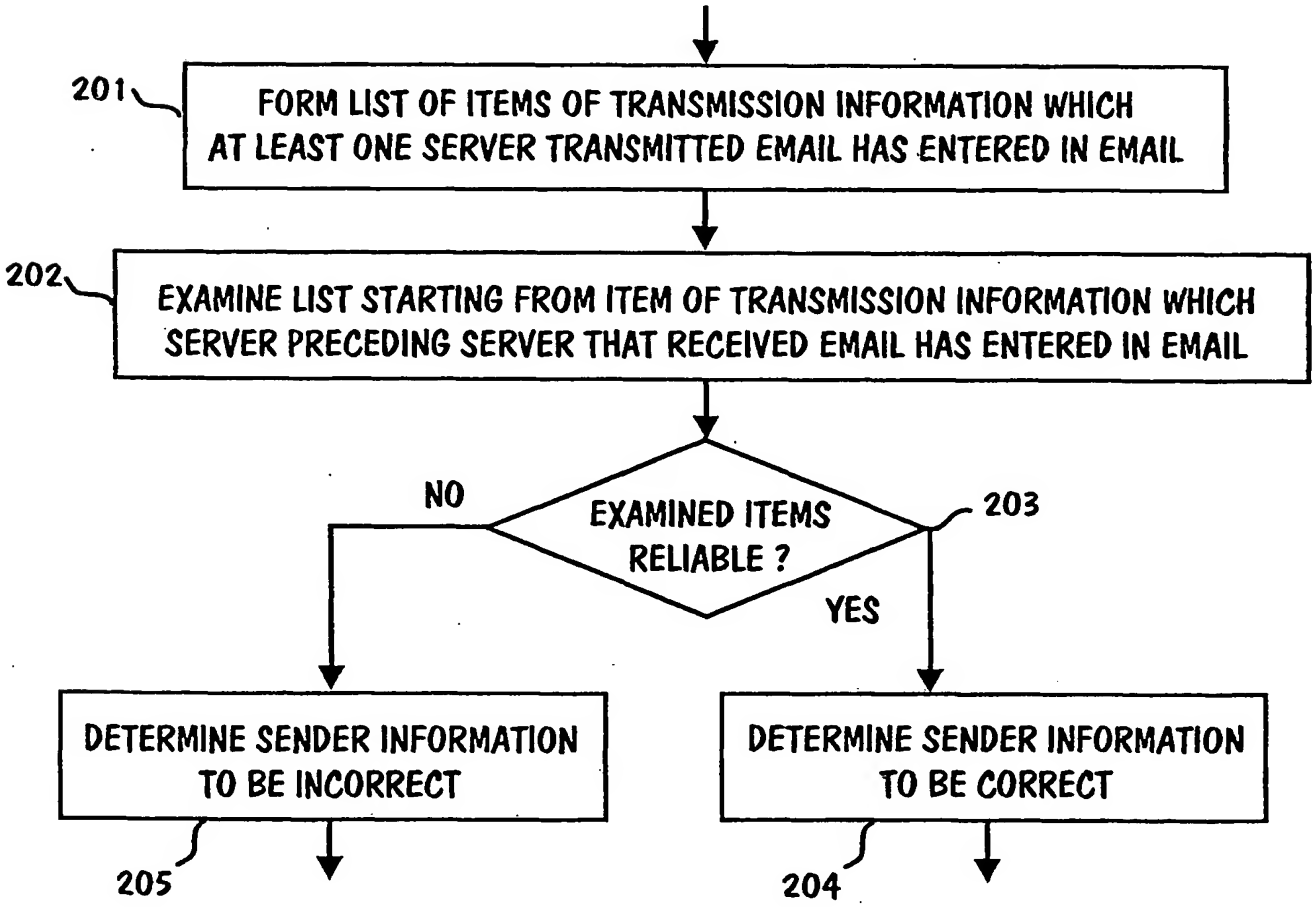


FIG. 2A

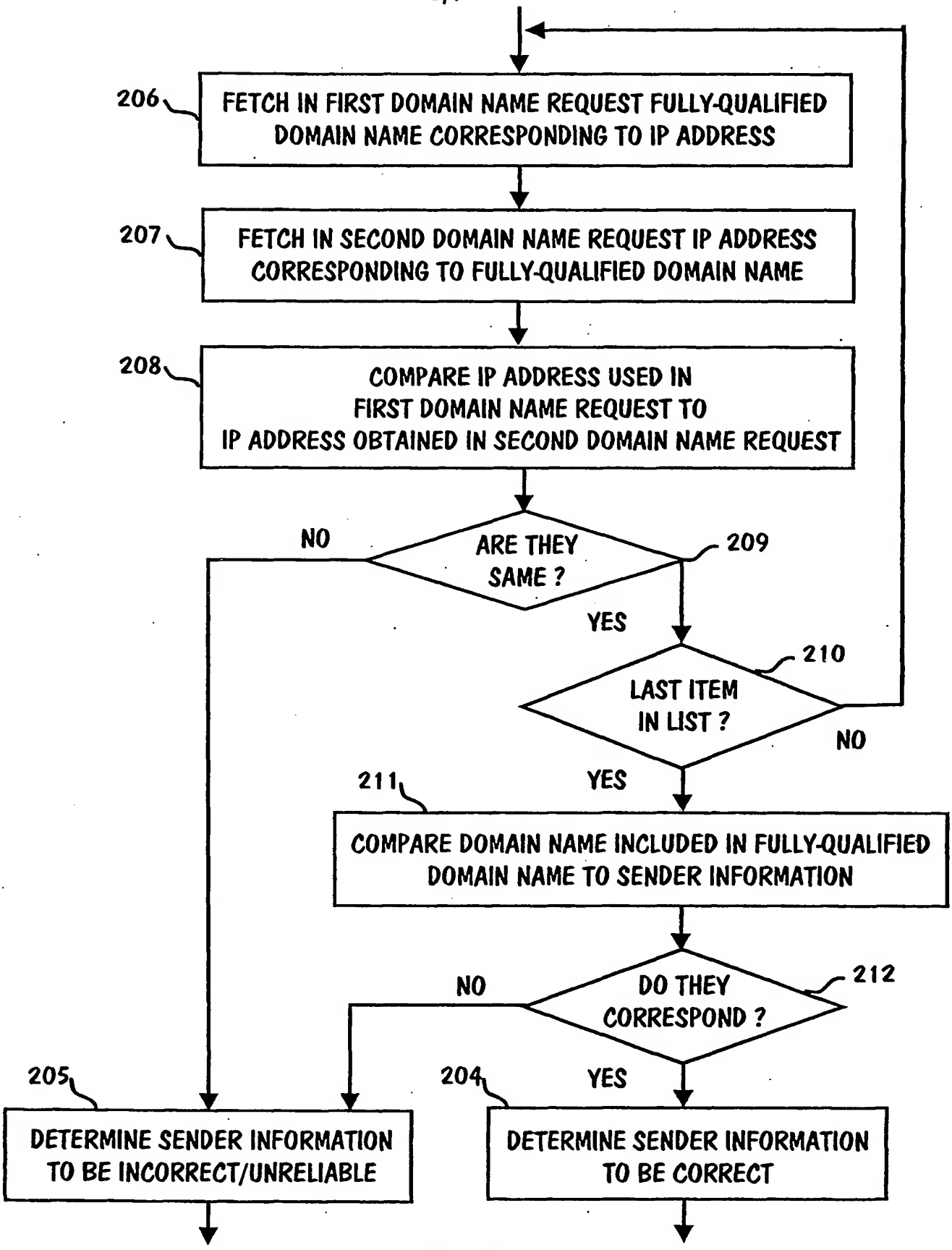

206
FETCH IN FIRST DOMAIN NAME REQUEST FULLY-QUALIFIED DOMAIN NAME CORRESPONDING TO IP ADDRESS
207
FETCH IN SECOND DOMAIN NAME REQUEST IP ADDRESS CORRESPONDING TO FULLY-QUALIFIED DOMAIN NAME
208
COMPARE IP ADDRESS USED IN FIRST DOMAIN NAME REQUEST TO IP ADDRESS OBTAINED IN SECOND DOMAIN NAME REQUEST
ARE THEY SAME ?
NO
209
YES
210
LAST ITEM IN LIST ?
NO
YES
211
COMPARE DOMAIN NAME INCLUDED IN FULLY-QUALIFIED DOMAIN NAME TO SENDER INFORMATION
DO THEY CORRESPOND ?
NO
212
YES
205
DETERMINE SENDER INFORMATION TO BE INCORRECT/UNRELIABLE
204
DETERMINE SENDER INFORMATION TO BE CORRECT

FIG. 2B

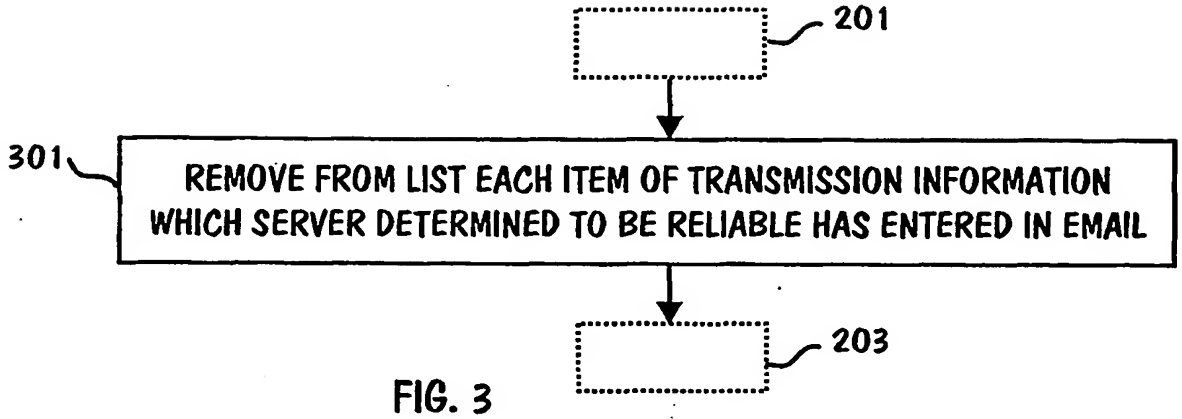


FIG. 3

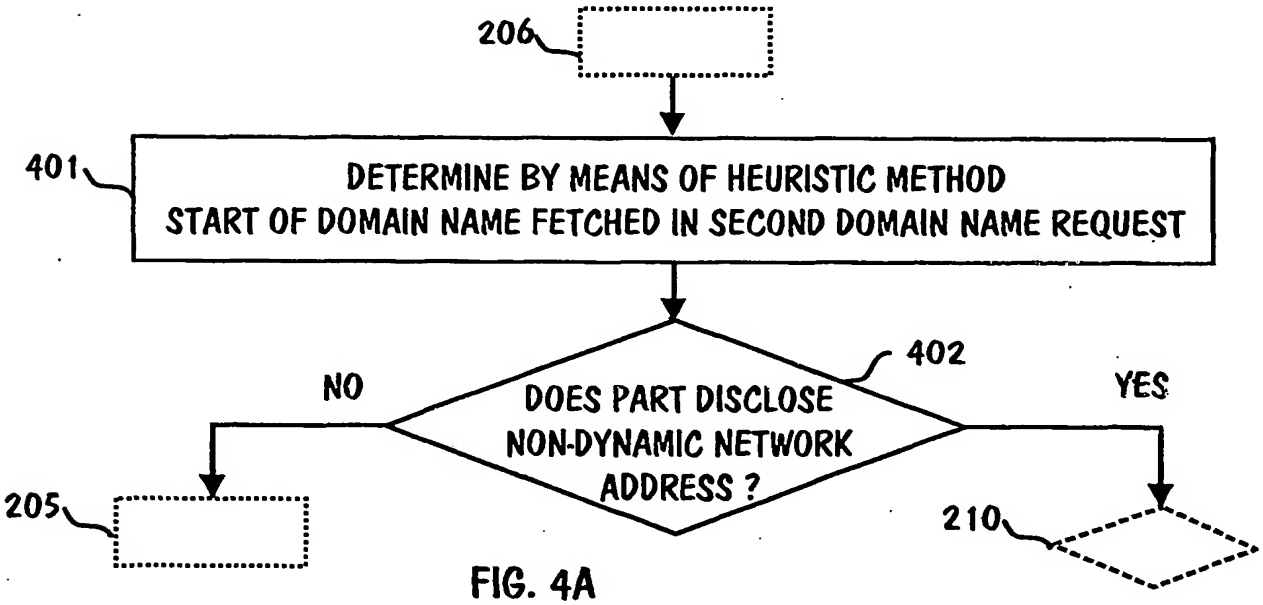


FIG. 4A

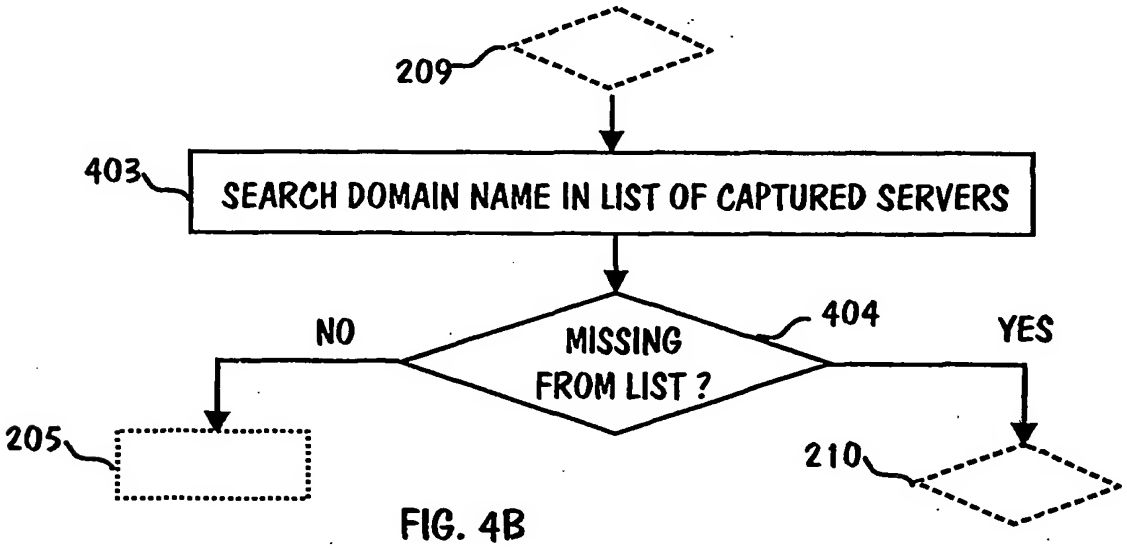


FIG. 4B

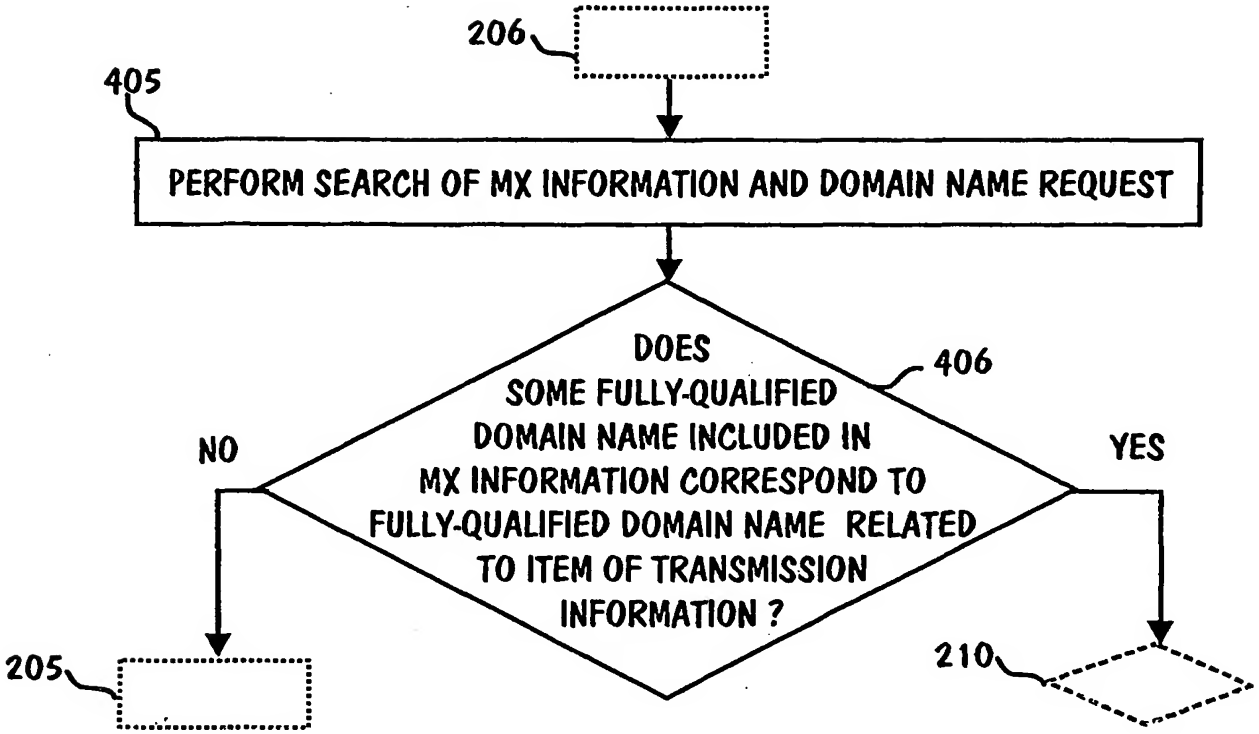

206
405
PERFORM SEARCH OF MX INFORMATION AND DOMAIN NAME REQUEST
DOES SOME FULLY-QUALIFIED DOMAIN NAME INCLUDED IN MX INFORMATION CORRESPOND TO FULLY-QUALIFIED DOMAIN NAME RELATED TO ITEM OF TRANSMISSION INFORMATION ?
406
NO
YES
205
210

FIG. 4C

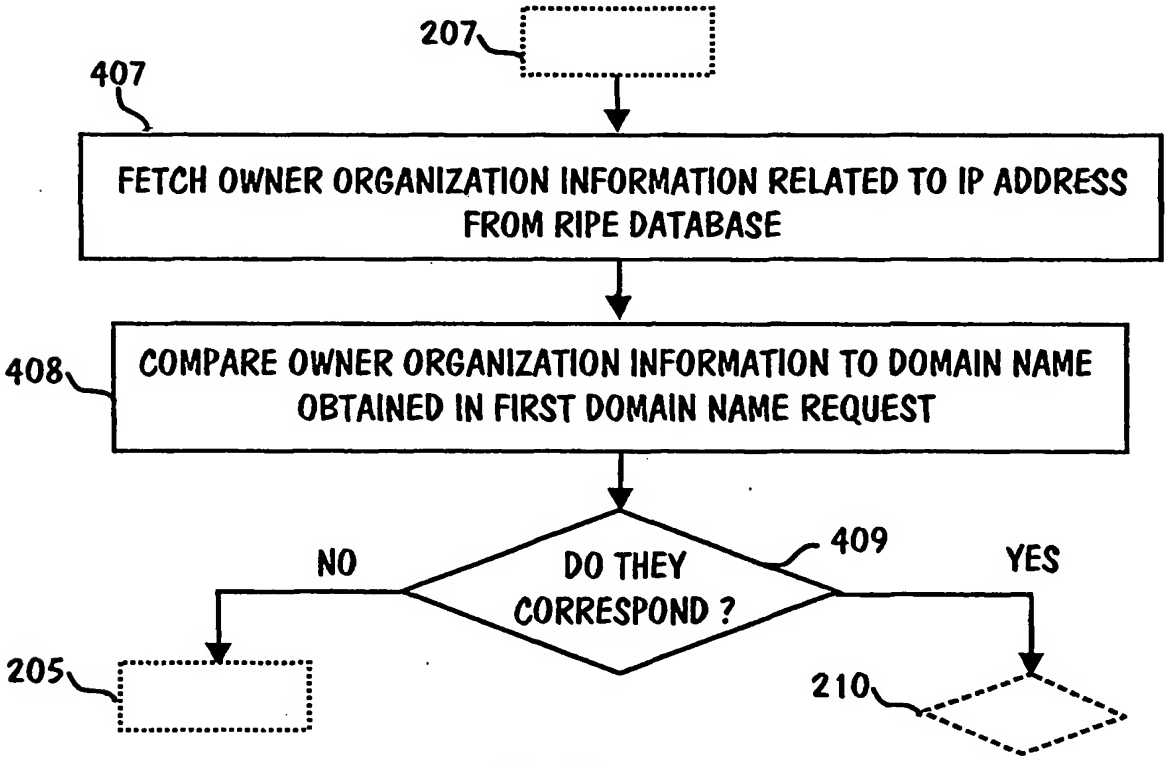

207
407
FETCH OWNER ORGANIZATION INFORMATION RELATED TO IP ADDRESS FROM RIPE DATABASE
408
COMPARE OWNER ORGANIZATION INFORMATION TO DOMAIN NAME OBTAINED IN FIRST DOMAIN NAME REQUEST
DO THEY CORRESPOND ?
409
NO
YES
205
210

FIG. 4D

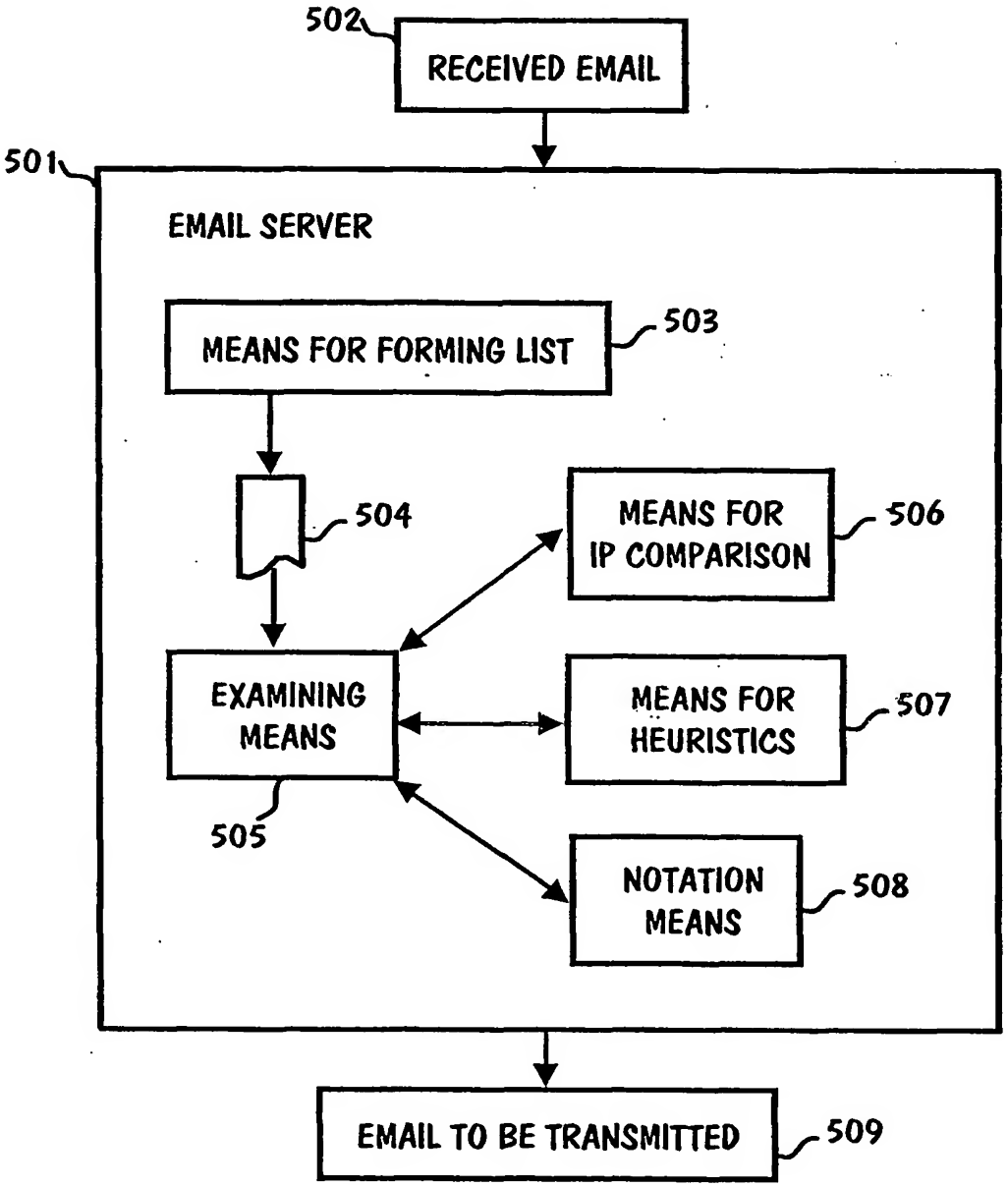

502
RECEIVED EMAIL
501
EMAIL SERVER
MEANS FOR FORMING LIST
503
504
MEANS FOR IP COMPARISON
506
EXAMINING MEANS
MEANS FOR HEURISTICS
507
505
NOTATION MEANS
508
EMAIL TO BE TRANSMITTED
509

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2006/050251

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC8: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0068542 A1 (LALONDE et al.) 08 April 2004 (08.04.2004), abstract and paragraphs 0034-0037	1-2, 9, 11-12, 14-15, 22
X	JP 2004064215 A (CASIO COMPUTER CO LTD) 26 February 2004 (26.02.2004), abstract and paragraph 0011 (computer translation)	1-2, 14-15
A	WO 2005/031586 A1 (BLUEBOTTLE SOLUTIONS PTY LTD et al.) 07 April 2005 (07.04.2005)	
A	WO 2004/081734 A2 (PROPEL SOFTWARE CORP) 23 September 2004 (23.09.2004)	
A	US 2002/0198950 A1 (LEEDS ROBERT G) 26 December 2002 (26.12.2002)	

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 August 2006 (22.08.2006)	11 September 2006 (11.09.2006)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Arto Anttila
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050251

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2004/0068542 A1	08/04/2004	CN 1703868 A	30/11/2005
		WO 2004034198 A2	22/04/2004
		EP 1550257 A2	06/07/2005
		AU 2003279852 A1	04/05/2004
JP 2004064215 A	26/02/2004	None	
WO 2005/031586 A1	07/04/2005	AU 2004276844 A1	07/04/2005
		EP 1676206 A1	05/07/2006
WO 2004/081734 A2	23/09/2004	EP 1604293 A2	14/12/2005
		US 2005091320 A1	28/04/2005
		US 2005080857 A1	14/04/2005
		US 2005091319 A1	28/04/2005
		US 2005080856 A1	14/04/2005
		US 2005080855 A1	14/04/2005
		US 2004177120 A1	09/09/2004
US 2002/0198950 A1	26/12/2002	US 2004249893 A1	09/12/2004
		US 2002016824 A1	07/02/2002

International application No.
PCT/FI2006/050251

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 12/58 (2006.01)